REMARKS

Claims 1, 4-26, 28-30, 32-42, and 44-48 are currently pending in the application. In view of the following remarks, Applicant respectfully requests withdrawal of the rejections and forwarding of the application onto issuance.

The § 102 Rejections

Claims 1, 4-26, 28-30, 32-42, and 44-48 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,708,274 to Herbert et al (hereinafter "Herbert").

Claim 1 recites, in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory, a computer-implemented method of protecting information comprising [emphasis added]:

- creating a key and page locking the key in the physical memory, wherein creating the key comprises creating the key during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups;
- encrypting information using the key; and
- paging out, to the page file, the encrypted information.

In making out the rejection of this claim, the Office cites columns 2, 3 and 4 of Herbert and argues that it teaches creating a key and page locking the key in the physical memory, creating the key during system boot up, and creating different keys during different system boot ups.

Applicant respectfully disagrees and traverses the Office's rejection. Applicant submits that the Office has mischaracterized these portions of Herbert's subject matter. Specifically, the excerpts cited by the Office do not disclose or

suggest that a key is created during ***system boot,*** wherein ***different*** keys can be created during ***different*** system boot ups. Applicant directs the Office's attention to column 4, lines 7-25, and column 6, lines 58-65, which teach that Herbert's key is generated ***at the time of software installation.*** Those excerpts are reproduced below [emphasis added]:

> At some time, software must be installed in the secure environment. Such "off the shelf" software will, of course, not be encrypted in the manner used within the secure environment. It will typically have a digital signature which can be used to verify the authenticity of the software being installed if digital signature verification is a supported function within the secure environment. FIG. 3 shows a flowchart of ***installation of a program*** in the secure system. ***At functional block 120, a key is generated*** and initialization vector is generated for an application to be installed. Key generation can be accomplished using the random number generator which generates random bits. Random bits are collected until the desired key length is reached. In one embodiment, the random number generator has a thirty-two bit output register. The processor 16 reads the register a number of times necessary to collect enough random bits for a full key. Keys can be generated with one key for each application, i.e. all code pages and data pages associated with one application share the same key. One concern with shared keys between pages is that if, for example, two data pages have identical content, they would generally encrypt to the same encrypted value. *Col. 4, lines 7-28.*

> As discussed above, ***the encryption key*** and IV are generated ***at the time of installation.*** *Col. 6, lines 59-60.*

Applicant respectfully submits that these excerpts teach that the key in Herbert is created ***at the time of software installation***. Furthermore, in contrast to ***different*** keys that can be created during ***different*** system boot ups, Herbert appears to utilize the ***same*** key(s) created for a given software application across ***multiple*** system boot ups.

When viewed in the context of the claimed subject matter, it becomes apparent that Herbert is really concerned with something that is quite different from the subject matter of this claim. Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claims 4-10 depend from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 11 recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- creating a key during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups;
- page-locking the key in main memory;
- restricting access to the page-locked key to only the operating system kernel;
- calling the operating system kernel to encrypt information;
- accessing the page-locked key with the operating system kernel; and
- using the operating system kernel to encrypt the information with the page-locked key.

In making out the rejection of this claim, the Office cites to the same excerpts of Herbert cited above.

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Applicant respectfully submits that the Office has mischaracterized those excerpts of Herbert, which do not disclose or suggest

creating a key during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claims 12-18 depend from claim 11 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 11, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 19 recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of handling encrypted information comprising [emphasis added]:

- accessing encrypted information in the page file; and
- decrypting the encrypted information with a key created during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups and wherein the key is page-locked in the main memory.

In making out the rejection of this claim, the Office cites to the same excerpts of Herbet as cited above. The Office argues that these excerpts teach decrypting the encrypted information with a key created during boot up, wherein different keys can be created during different system boot ups and wherein the key is page-locked in the main memory.

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Herbert does not teach that a key is created during ***system boot***

up, wherein different keys can be created during ***different*** system boot ups, as claimed.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claims 20-24 depend from claim 19 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 19, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 25 recites, in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- allocating a non-pageable page of main memory during system boot;
- generating a random key, wherein ***different*** keys can be generated during ***different*** system boots; and
- storing the random key in the non-pageable page of main memory, the random key being configured for use by the operating system to encrypt information that might be paged out to the page file.

In making out the rejection of this claim, the Office argues that the above-cited excerpted portions of Herbert teach "generating a random key, wherein different keys can be generated during different system boots".

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Applicant respectfully submits that the Office has mischaracterized the excerpts of Herbert, which do not teach that ***different*** keys can be generated during ***different*** system boots.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claims 26, 28 and 29 depend from claim 25 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 25, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 30 recites, in an operating system having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information comprising [emphasis added]:

- generating at least one non-pageable random key by using a random key generation process during ***system boot up***, wherein ***different*** keys can be generated during ***different*** system boot ups;
- encrypting at least one selected block of information in the main memory with a software component that uses the at least one random key for encryption;
- transferring the one encrypted block of information to the secondary storage;
- decrypting the one encrypted block of information with the software component that uses the at least one random key for decryption; and
- placing the decrypted block of information in the main memory.

In making out the rejection of this claim, the Office cites to the same excerpts of Herbert and argues that these excerpts teach generating at least one non-pageable random key by using a random key generating process during system boot up, wherein different keys can be generated during different system boot ups.

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Applicant respectfully submits that the Office has mischaracterized these excerpts of Herbert, which do not teach using a random key generating process during ***system boot up***, wherein ***different*** keys can be generated during ***different*** system boot ups.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claims 32-35 depend from claim 30 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 30, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 36 recites a system for use in protecting pageable information comprising [emphasis added]:

- a memory having pageable and non-pageable pages; and
- at least one key created during ***system boot*** and stored in the memory in a non-pageable page, the key being configured for use in encrypting pageable information, wherein ***different*** keys can be created during ***different*** system boots.

In making out the rejection of this claim, the Office again cites to the same excerpts of Herbert and argues that these excerpts teach at least one key created during system boot and stored in the memory in a non-pageable page, the key being configured for use in encrypting pageable information, wherein different keys can be created during different system boots.

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Applicant respectfully submits that the Office has

mischaracterized these excerpts of Herbert, which do not teach or suggest the subject matter of this claim.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claims 37-40 depend from claim 36 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 36, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 41 recites a computer program embodied on one or more computer-readable media, the program comprising [emphasis added]:

- creating a key and page locking the key in main memory of a computer, wherein creating the key comprises creating the key during ***system boot up, wherein different keys can be created during different*** system boot ups;
- encrypting information with the key;
- paging out, to secondary storage, the encrypted information;
- accessing the encrypted information in the secondary storage; and
- decrypting the encrypted information with the key that is page-locked in the main memory.

In making out the rejection of this claim, the Office cites to the same excerpts of Herbert and argues that these excerpts teach creating a key and page locking the key in main memory of a computer, wherein creating the key comprises creating the key during system boot up, wherein different keys can be created during different system boot ups.

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Applicant respectfully submits that the Office has

mischaracterized these excerpts of Herbert, which do not teach creating the key during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claim 42 recites a programmable computer comprising [emphasis added]:

- a processor;
- main memory for holding information;
- secondary storage for receiving information that is temporarily transferred out of the main memory;
- the computer being programmed with computer-readable instructions which, when executed by the processor, cause the computer to:
  - generate a key during ***system boot up***, wherein ***different*** keys can be generated during ***different*** system boot ups;
  - page lock the key in the main memory;
  - encrypt information that is to be transferred to the secondary storage with the key;
  - transfer the encrypted information to the secondary storage; and
  - decrypt the encrypted information with a key that is locked in the main memory.

In making out the rejection of this claim, the Office cites to the same excerpts of Herbert and argues that these excerpts teach generating a key during system boot up, wherein different keys can be generated during different system boot ups.

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Applicant respectfully submits that the Office has mischaracterized these excerpts of Herbert, which do not teach generating a key

during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claims 44-46 depend from claim 42 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 42 are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 47 recites one or more application programming interfaces embodied on one or more computer-readable media for execution on a computer in conjunction with a paging operating system having main memory for holding information and a page file for receiving information that is paged out from the main memory, comprising [emphasis added]:

- an interface method for generating a key during ***system boot up***, wherein ***different*** keys can be generated during ***different*** system boot ups;
- an interface method for page locking the key in the main memory,
- an interface method for encrypting pageable information with the key; and
- an interface method for decrypting encrypted information that is contained in the page file.

In making out the rejection of this claim, the Office cites to the same excerpts of Herbert and argues that the excerpts teach generating a key during system boot up, wherein different keys can be generated during different system boot ups.

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Applicant respectfully submits that the Office has mischaracterized these excerpts of Herbert, which do not teach generating a key during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Claim 48 recites an application programming interface embodied on a computer-readable medium for execution on a computer in conjunction with a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory, comprising a method for setting an attribute on a page of main memory, the attribute designating that the page must be encrypted with a key created ***during system boot up*** and page-locked in the main memory prior to the page being paged out to the page file, wherein ***different*** keys can be created during ***different*** system boot ups.

In making out the rejection of this claim, the Office argues that columns 1-4 teach a key created during system boot up and locked in the main memory prior to the page being paged out to the page file, wherein different keys can be created during different system boot ups.

Applicant respectfully disagrees and traverses the Office's rejection. As discussed above, Herbert does not teach a key created during ***system boot up***, wherein ***different*** keys can be created during ***different*** system boot ups.

Accordingly, since Herbert does not disclose or suggest the subject matter of this claim, this claim is allowable.

Conclusion

Applicant has sincerely attempted to address the Office's rejections and advance prosecution in this matter. The Office, however, continues to maintain its position with regard to what it believes Herbert discloses. Applicant would like to avoid the time and expense of having to file an appeal in this application to advance prosecution. However, Applicant believes that this may be an inevitability. Accordingly, the Office is respectfully urged to contact the undersigned, prior to issuing an Advisory Action, to discuss this application and hopefully advance prosecution short of an appeal.

All of the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of discussing an appeal.

Respectfully Submitted,

Dated: 3/29/05

By: _____

Lance R. Sadler
Reg. No. 38,605
(509) 324-9256